

## **The Formation of the National OPSEC Standard**

After the Vietnam era and the successes of Operation PURPLE DRAGON, a significant ripple effect was felt throughout the intelligence, military, and government sectors. The focus had deviated from solely protecting classified information to protecting unclassified data due to its propensity to reveal information about sensitive operations or systems. Agencies within the United States began to consider a more world-centric view of OPSEC, especially in regards to the abilities of foreign surveillance apparatuses. By applying the principles learned in PURPLE DRAGON, national security entities could enable greater security of classified mission operations; they could also more effectively curb the ability of the enemy to develop strategies to compromise U.S. interests around the globe.

With the increasing necessity to protect unclassified information, the new sophistication of the Soviet Empire and the ramifications of the GUNMAN debacle, then President Reagan signed National Security Decision Directive (NSDD) 298 on 22 January 1988. NSDD 298 established community standards throughout the government to ensure that all unclassified information related to national security efforts would be reviewed prior to release. Although security programs and procedures already existed to protect classified information, this was the first formal national-level program designated to protect unclassified information.

From the directive, executive departments and agencies that supported national security missions would be mandated to establish a formal OPSEC program, and the minimum common features were codified into the following:

- Specific assignment of responsibility for OPSEC direction and implementation.
- Specific requirements to plan for and implement OPSEC in anticipation of and, where appropriate, during department or agency activity.
- Direction to use OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures.
- Enactment of measures to ensure that all personnel commensurate with their positions and security clearances are aware of hostile intelligence threats and understand the OPSEC process.
- Annual review and evaluation of OPSEC procedures so as to assist the improvement of OPSEC programs.
- Provision for interagency support and cooperation with respect to OPSEC programs.

While those agencies with minimal activities affecting national security were not mandated to establish formal OPSEC programs, they were required to cooperate with other departments and agencies to help minimize damage to national security if problems arose. NSDD 298 designated the Director of the National Security Agency to be the Executive Agent for interagency OPSEC training and furthermore mandated the NSA to assist executive departments and agencies to establish OPSEC programs, develop and provide interagency OPSEC training courses, and establish and maintain an Interagency OPSEC Support Staff. The OPSEC mandate founded IAD's IOSS and made them responsible to:

- Carry out interagency, national-level, OPSEC training for executives, program and project managers, and OPSEC specialists;
- Act as consultant to Executive departments and agencies in connection with the establishment of OPSEC programs and OPSEC surveys and analyses; and
- Provide an OPSEC technical staff.

Through the NSDD 298, the U.S. Government officially forged a change in the practices and procedures of all national security entities, both foreign and domestic. With the formation of the IOSS and the NSA directive to lead the national OPSEC program, the government established a sound foundation in which future operations and strategies would be better protected. The United States' adherence to these guidelines have not only saved lives, but protected the information and systems that provide for our continued success as a nation and world power.